Claims 1-24, all the claims pending in the application, stand rejected on prior art grounds. Claims 1-24 also stand rejected under 35 U.S.C. §101. Claim 7 is objected to. Applicants respectfully traverse these rejections based on the following discussion.

I.   The Objection Of Claim 7

The Examiner objected claim 7 because of a period at the end of line 4; however, claim 7 is not amended herein because as the claim is presently presented there does not appear to be a period at the end of line 4.

II.   The 35 U.S.C. §101 Rejection Of All Claims

The Office Action again rejects claims 1-24 under 35 U.S.C. §101 for being directed to non-statutory subject matter. Specifically, the Office Action provides that claims are directed to methods etc., but that the "methods claimed appear to be directed towards abstract ideas and do not produce a useful, concrete and tangible result." The Applicants traverse these rejections because the computer-implemented method of "mining for association rules" necessarily produces a useful, tangible and concrete result: a new and different randomized dataset which in turn allows recovery of an association rule while controlling privacy breaches of individual transactions.

Specifically, as the amount of personal information contained in digital databases increases, privacy concerns have also increased (see paragraph [0006]). These concerns extend to tools, such as data mining, that are used to efficiently recover valuable, non-obvious

information (e.g., association rules) from the databases (see paragraph [0004] of the specification). The present invention, as defined in amended independent claims 1, 7, 13, and 19, discloses a computer-implemented method of data mining for association rules, while simultaneously controlling privacy breaches of individual transactions within the databases (see paragraphs [0027-0028] and [0038-0043]).

This method does not solely comprise performing a mathematical algorithm on a dataset. Rather it comprises taking an original dataset and producing a second new and different randomized data set by randomly dropping true items from each transaction in the original dataset as well as randomly inserting false items into each transaction in the original dataset. Then, the nonrandomized support of an association rule in the original dataset is estimated based on the randomized support of that association rule in the randomized dataset in order to recover the association rule and control privacy breaches of the individual transactions. The Federal Circuit in Arrhythmia Research Tech., Inc. v. Corazonix Corp., 958 F. 2d 1053, 22 USPQ 2d 1033 (Fed. Cir. 1992) at 1039 held that a claimed invention was statutory subject matter under §101 because: "The computer-performed operations transform a particular input signal to a different output signal, in accordance with the internal structure of the computer as configured by electronic instructions. 'The claimed invention … converts one physical thing into another physical thing just as any other electrical circuitry would do.'" Thus, the useful, tangible and concrete result of the present invention is a new and different randomized dataset which in turn allows the recovery of an association rule that preserves the privacy of individual transactions (see paragraph [0034]). That is, the claimed method of the present invention is statutory subject

matter because the computer-performed operations transform a particular dataset (i.e., one physical thing) into a different data set (i.e., another physical thing).

The Applicants note that all claims, as amended, are properly supported in the specification and accompanying drawings, and no new matter is being added. In view of the foregoing, the Examiner is respectfully requested to reconsider and withdraw the rejections.

III. Prior Art Rejections

Claims 1-24 stand rejected under 35 U.S.C. §102(a) as being anticipated by Evfimievski ("Randomization in Privacy Preserving Data Mining," December 2002, ACM SIGKDD Eplorations Newsletter, Vol. 4, Issue 2, pp. 43-48) hereinafter referred to as Randomization in Privacy Preserving Data Mining (see **Attachment A to Exhibit 1**). Applicants respectfully traverse these rejections based on the following discussion and Exhibit 1 which is a declaration under 37 C.F.R §1.132.

MPEP §2132.01 provides that the "Applicant's disclosure of his or her own work within the year before the application filing date cannot be used against him or her under 35 U.S.C. 102(a). *In re Katz*, 687 F.2d 450, 215 USPQ 14 (CCPA 1982) (discussed below). Therefore, where the applicant is one of the co-authors of a publication cited against his or her application, the publication may be removed as a reference by the filing of affidavits made out by the other authors establishing that the relevant portions of the publication originated with, or were obtained from, applicant. Such affidavits are called disclaiming affidavits. *Ex parte Hirschler*, 110 USPQ 384 (Bd. App. 1952)."

It is the Applicants position that those portions of the cited prior art (i.e., Randomization in Privacy Preserving Data Mining) that disclose the claimed features of the invention are

actually derived from and reference another paper (Evfimievski, R. Srikant, R. Agrawal and J. Gehrke, "Privacy Preserving Mining of Association Rules," Proc. Of 8th ACM SIGKDD Intl. Conf. on Knowledge Discovery and Data Mining (KDD), July 2002, herinafter referred to as Privacy Preserving Mining of Association Rules (**see Attachment B to Exhibit 1**). Furthermore, Privacy Preserving Mining of Association Rules is the Applicant's own work and was published within the year before the filing date of the present application. The disclaiming affidavit presented in Exhibit 1 and signed by two of three Applicants supports the fact that Privacy Preserving Mining of Association Rules is the Applicants's own work, despite the additional author, J. Gehrke. Thus, any portions of Randomization in Privacy Preserving Data Mining that were derived from Privacy Preserving Mining of Association Rules are not available as prior art against the present application under 35 U.S.C. 102(a).

More particularly, in response to the §102(a) rejection of claims 1-24 in the previous Office Action, the Applicants submitted disclaiming affidavits (i.e., declarations) signed by both Alexandre Evfimievski and J. Gehrke. However, the Examiner found that these declarations were insufficient to overcome the rejection for the following reasons: (1) they were not properly executed because they were not signed by all inventors; (2) they did not establish that the reference is a publication of the Applicants' own work; (3) they did not provide sufficient facts and documentary evidence supported by actual proof; and (4) they did not refer to the claims, prior to the date of the reference.

As to proper execution of the affidavits, the Applicants submit that signatures by all of the inventors are not required. Specifically, the Office Action cites MPEP§715.04 as support for the position that all inventors must sign the supporting affidavits. The Applicants respectfully

disagree based on the following discussion. MPEP§715.04 sets out the formal requirements for parties making an affidavit or declaration under 37 C.F.R. §1.131. 37 C.F.R. §1.131 provides that declarations "to establish invention of the subject matter of the rejected claim prior to the effective date of the reference must be signed by all inventors." However, the declarations of Andre Evfimievski and Johannes Gehrke that were filed in conjunction with the Applicants' response to the first office action were not for the purpose of swearing behind the cited references under 37 C.F.R. §1.131. Rather the declarations of Andre Evfimievski and Johannes Gehrke were filed in order to establish attribution. That is, MPEP§716.10 discusses attribution and indicates that a declaration under 37 C.F.R. §1.132 may be filed to show that "the reference discloses subject matter derived from the applicant ...". Declarations filed under 37 C.F.R. §1.132 do not require the signature of all inventors (i.e., 1.132 simply indicates that "any evidence submitted to traverse the reject ... must be by way of an oath or declaration."). Neither the MPEP, nor the rules set out in the C.F.R., indicate specifically who may make an oath or declaration under 37 C.F.R. §1.132. It should be noted that because declarations under 37 C.F.R. §1.131 require the signature of all inventors, MPEP§715.04 further includes exceptions to this rule, for example, to overcome situations in which not all inventors are available.

As to the other reasons for insufficiency set out by the Examiner, Exhibit 1, a revised declaration under 37 C.F.R. §1.132, is provided. This revised declaration sets out with greater specificity how those portions of the <u>Randomization in Privacy Preserving Data Mining</u> that disclose the features of claims 1-24 are actually derived from another reference (i.e., <u>Privacy Preserving Mining of Association Rules</u>) that is the Applicant's own work and is dated within the year before the application date such that <u>Randomization in Privacy Preserving Data Mining</u>

is not proper to be used against the present application under 35 U.S.C. 102(a), as discussed below. Alexandre Evfimievski, Ramkrishnan Srikant and Rakesh Agrawal are the inventors of the present invention and were all employees of of the Assignee, International Business Machines, Inc. (IBM), at the time of the invention. However, Rakesh Agrawal is no longer an employee of IBM and all attempts made to contact him in order to obtain his signature have proved futile. Thus, Exhibit 1 is signed only by Alexandre Evfimievski and Ramkrishnan Srikant. However, as discussed above, since Exhibit 1 is a declaration under 37 C.F.R. §1.132 and 37 C.F.R. §1.131, Rakesh Agrawal's signature is not required.

More specifically, Exhibit 1 is offered to show the following.

Randomization in Privacy Preserving Data Mining is an overview of research in the field of privacy preserving data mining and is derived from several papers. This paper "presents some methods and results in randomization for numerical and categorical data and discusses the issue of measuring privacy" (see Abstract). Portions of Randomization in Privacy Preserving Data Mining were derived from and directly reference the following paper:Each of the Applicants of the present invention are co-authors on Privacy Preserving Mining of Association Rules along with J. Gehrke. Privacy Preserving Mining of Association Rules describes the invention defined by claims 1-24 and, specifically, was the paper on which the present application was based. The present application was filed within 1 year of the date of publication of Privacy Preserving Mining of Association Rules.

J. Gehrke was a professor and advisor of A. Evfimievski, during the time period in which the idea for the invention was conceived. Although J. Gehrke is listed as a co-author of Privacy Preserving Mining of Association Rules, he was not an inventor. It is a common practice for

professors/advisors to be listed as co-authors on published papers of student, regardless of whether they meet the technical criteria for being considered an "inventor," as defined by the USPTO. Additionally, J. Gehrke has read U.S. Patent Application Serial No. 10/624,069 and has declared that he is not an inventor of the invention defined by claims 1-24 (see Attachment C to Exhibit 1). The fact that J. Gehrke has declared that he himself is not an inventor of the claimed invention should be sufficient to establish this fact. However, Alexandre Evfimievski and Ramkrishnan Srikant further acknowledge and declare that J. Gehrke was not an inventor of the invention defined by claims 1-24 (see Exhibit 1). Therefore, the portions of Privacy Preserving Mining of Association Rules that describe the features of claims 1-24 describe the Applicants' own work and no one else's and predates the cited prior art.

Regarding the rejected claims 1-24, the Office Action provides that Randomization in Privacy Preserving Data Mining anticipates all of the various claimed features of the invention. However, many of the cited portions of Randomization in Privacy Preserving Data Mining are not the original work of A. Evfimievski, but rather were derived from the paper Privacy Preserving Mining of Association Rules, which, as discussed above, describes the Applicants' own work. Therefore, it necessarily follows that the cited portions of Randomization in Privacy Preserving Data Mining, which the Office Action indicates as disclosing the features of claims 1-24, were also derived from the Applicants' own work. Consequently, the cited portions of Randomization in Privacy Preserving Data Mining are not available as prior art against the present application (see above discussion of MPEP §2132.01).

More specifically, the following portions <u>Randomization in Privacy Preserving Data Mining</u> cited in the Office Action were derived from the following portions of <u>Privacy Preserving Mining of Association Rules</u> and are, therefore, the Applicants' own work.

A. P. 43, left column, paragraph 3, lines 10 – right column, paragraph 1, line 2; p. 44, right column, paragraph 6, lines 2-4; and p. 45, left column, paragraph 4, lines 7-8 of <u>Randomization in Privacy Preserving Data Mining</u> were each cited as disclosing both the feature of "randomly dropping true items from each transaction in said original dataset" and the feature of "randomly inserting false items into each transaction in said original data set." Specifically, regarding p. 43, left column, paragraph 3, lines 10 – right column, paragraph 1, line 2, no specific reference is credited by Evfimievski for the cited sentence. However, the idea of "before sending its piece of data, each client perturbs it so that some true information is taken away and some false information is introduced" is derived directly from the statement "… in addition to replacing some of the items, we shall insert so many "false" items into a transaction that one is as likely to see a "false itemset as a "true" one", which is found in the second sentence of section 4 of <u>Privacy Preserving Mining of Association Rules</u>. Regarding p. 44, right column, paragraph 6, lines 2-4, no specific reference is credited by Evfimievski for the cited sentence. The first sentence in paragraph 6 that immediately precedes the cited lines refers specifically to <u>Privacy Preserving Mining of Association Rules</u> along with another reference, the publication date of which is later (i.e., August 2002). Additionally, this sentence, "Suppose that each client C_i has a transaction t_i, which is a subset of a given finite set of items I, $|I| = n$" does not

amount to "randomly dropping true items from each transaction in said original dataset" or "randomly inserting false items into each transaction in said original data set", but rather defines the transaction prior to randomly dropping true items therefrom. Regarding p. 45, left column, paragraph 4, lines 7-8, again no specific reference is credited by Evfimievski for the cited sentence; however, the sentence immediately following explains the statement and does credit <u>Privacy Preserving Mining of Association Rules</u>. Additionally, the idea of a "natural way to randomize a set of items is by deleting some items and inserting some new items is derived directly from the statement "… in addition to replacing some of the items, we shall insert so many "false" items into a transaction that one is as likely to see a "false" itemset as a "true" one" (see second sentence of section 4 of "Privacy Preserving Mining of Association Rules" (July 2002)).

B. P. 45, left column, paragraph 8, lines 1-3 of <u>Randomization in Privacy Preserving Data Mining</u> is cited in the Office Action as disclosing the features of "creating a randomized dataset by collecting said randomized transactions" and of "collecting said randomized dataset in a database." Again, no specific reference is credited by Evfimievski for the cited sentence, which states "In the set T' of randomized transactions available to the server, itemsets have supports very different from their supports in the nonrandomized dataset T." However, this sentence is contained within a section of the paper that comprises a summary <u>Privacy Preserving Mining of Association Rules</u> and, specifically, a summary of section 4 of the article. More

specifically, the idea of "creating a randomized dataset by collecting said randomized transactions" is derived directly from Definition 5 of Section 4.1 of "Privacy Preserving Mining of Association Rules" (July 2002). That is, randomization R is "a per-transaction randomization if, for $T = (t_1, t_2, \ldots t_N)$, we can represent R(T) as R(t_1, $t_2, \ldots t_N$) = (R(1, t_1), R(2, t_2), \ldots, R(N, t_N)), where R(i, t) are independent random variables whose distributions depend only on t (and not on i). We shall write t'_i = R(i, t_i) = R(t_i)." It should be noted that the cited sentence on p. 45, left column, paragraph 8, lines 1-3 does not refer at all to collecting a randomized dataset in a database.

C. P. 45, left column, paragraph 9- right column, paragraph 6, line 9 of <u>Randomization in Privacy Preserving Data Mining</u> is cited in the Office Action as teaching the feature of "mining said database to recover an association rule after said dropping and inserting processes by estimating nonrandomized support of said association rule in said original dataset based on randomized support for said association rule in said randomized dataset, wherein due to said creating of said randomized transactions, privacy breaches of said individual transactions are controlled during said mining." This portion of <u>Randomization in Privacy Preserving Data Mining</u> specifically references <u>Privacy Preserving Mining of Association Rules</u> and is derived from Sections 4.3 and 4.4.

D. P. 45, left column, paragraph 4, line 13- paragraph 8, line 11 of <u>Randomization in Privacy Preserving Data Mining</u> is cited in the Office Action as teaching the feature of "wherein said process of creating randomized transactions comprises per transaction randomizing, such that randomizing operators are applied to each transaction independently." This portion of <u>Randomization in Privacy Preserving Data Mining</u> specifically references <u>Privacy Preserving Mining of Association Rules</u> and is derived directly from Sections 4.1.

E. P. 45, left column, paragraph 4, line 7- paragraph 8, line 11 is cited in the Office Action as teaching the feature of "wherein said process of creating randomized transactions is item-invariant such that a reordering of said transactions does not affect outcome probabilities." Again, this portion of <u>Randomization in Privacy Preserving Data Mining</u> specifically references <u>Privacy Preserving Mining of Association Rules</u> and is derived directly from Remark 1 of Section 4.1.

F. P. 46, left column, paragraph 3, lines 1-13 of <u>Randomization in Privacy Preserving Data Mining</u> is cited as teaching the features of "wherein said dropping of said true items and said inserting of said false items are carried out to an extent such that the chance of finding a false itemset in a randomized transaction relative to the chance of finding a true itemset in said randomized transaction is above a predetermined threshold" and "wherein said predetermined threshold provides that the chance of finding a false itemset in said randomized transaction is approximately equal to the

chance of finding a true itemset in said randomized transaction." Again, this portion of <u>Randomization in Privacy Preserving Data Mining</u> specifically references <u>Privacy Preserving Mining of Association Rules</u> and is derived from the second sentence in Section 4 and Section 4.1.

G. P. 45, left column, paragraph 8, line 1- paragraph 9, line 33 of <u>Randomization in Privacy Preserving Data Mining</u> is cited as teaching the feature of "wherein said process of creating randomized transactions is performed independently on said transactions prior to the transactions being collected in said database." No specific reference is credited by Evfimievski for the cited sentence. However, this sentence is contained within a section of <u>Privacy Preserving Mining of Association Rules</u> that does refer to and summarize "randomization" as described in "<u>Randomization in Privacy Preserving Data Mining</u>.

The Applicants further submit that the declaration of Exhibit 1 offered in response to the §102 rejection of claims 1-24 is properly executed, establishes that the reference is a publication of the Applicants' own work, provides sufficient facts and documentary evidence supported by actual proof, refers to the claims, prior to the date of the reference, and, thereby, overcomes the rejection. Moreover, the Applicants note that all claims are properly supported in the specification and accompanying drawings, and no new matter is being added. In view of the foregoing, the Examiner is respectfully requested to reconsider and withdraw the rejections.

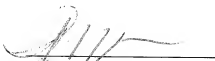### III. Formal Matters and Conclusion

In view of the foregoing, the Examiner is respectfully requested to reconsider and withdraw the rejections to the claims.

In view of the foregoing, Applicants submit that claims 1-24, all the claims presently pending in the application, are patentably distinct from the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary. Please charge any deficiencies and credit any overpayments to Attorney's Deposit Account Number 09-0441.

Respectfully submitted,

Dated: 9/26/06

Pamela M. Riley
Registration No. 40,146

Gibb I.P. Law Firm, LLC
2568-A Riva Road, Suite 304
Annapolis, MD 21401
Voice: (410) 573-0227
Fax: (301) 261-8825
Customer Number: 29154